REMARKS

Applicant respectfully requests reconsideration of this application, as amended, and consideration of the following remarks. Claims 1 and 18 have been amended. Claims 1, 3-6, 8-14 and 16-23 remain pending.

Amendments

Applicant has amended the claims to more particularly point out what Applicant regards as the invention. No new matter has been added as a result of these amendments.

Rejections

Rejections under 35 U.S.C. §103(a)

Claims 1, 3-5, 8-14, 17-18 and 20-23 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Edinger (US Pat Pub 2002/0194047) in view of Levi (US Pat 6,833,787) further in view of Thompson (US Pat Pub 2003/0061104).

Claim 6 stands rejected under 35 U.S.C. 103(a) as being unpatentable over Edinger in view of Levi, further in view of Thompson and further in view of Hughes (US Pat 4,535,204).

Claims 16 and 19 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Edinger in view of Levi, further in view of Thompson and further in view of Weiss (US Pat Pub 2002/0178364).

Applicant respectfully traverses these rejections as set forth in more detail below.

Edinger discloses a customer support management system and method that resolves both hardware and software problems using a single business model. The system and method is based on interaction between a hierarchy of corporate personnel/consultants and a customer support management system which tracks the evolution of customer support requests from inception to completion. The customer support management system includes a number of software tools including an automated scheduler connected to a database system for storing at least one of customer, product, service provider, and routing information. When a customer

experiences a problem with a hardware or software product, the customer sends a support request to the manufacturer. Through an interactive process, first, between the manufacturer and the customer and, then, between system personnel, the system tools are utilized to locate a service provider anywhere in the world in order to provide on-site support for satisfying the customer support request.

The Levi reference discloses a user contracts for service with an operations center (12) in order to provide monitoring and tracking services for a plurality of devices (30). After contracting for service, the operations center provides an agent (81) for download by a user to one or more of the user's devices (14, 16, 18, 20, 22, 630) for which the user has contracted for service. The agent is installed on the devices associated with the user's sites and communicates with the operations center. A listening process (710) at the operations center listens for periodically sent beacon packets (640) generated by a monitored device (630). Using location indicators included with the beacon packets and generated by an agent (681) on the monitored device, the operations center provides notifications (712) to a handler regarding the location of the monitored device if the monitored device is reported as stolen. A tracking response (714) may be communicated to the monitored device to take special actions when the device is stolen and to update the agent and other portions of the monitored device.

The Thompson reference discloses a warranty support for purchased products is provided by an electronic warranty administrator that maintains a plurality of databases. A first database identifies customers, either individuals or corporate entities having warranted products. A second database identifies the manufacturers of those products. The warranty administrator coordinates between the customer, the manufacturer and a service provider to provide warranty repairs. Unlike conventional extended warranties offered by third parties, the manufacturer remains in the repair process and thereby gains valuable information about the long term satisfaction of the customers. The warranty administrator also provides the manufacturer with a means to contact the customer about other products, product recalls and affinity programs thereby promoting brand loyalty.

The Lawrence reference discloses a data processing system having a pair of mirrored storage units maintains a state record of the mirrored pair in system memory.

In order to be able to determine state when the system is re-initialized, this state information is also stored on each storage unit of the mirrored pair, and in an alternate location. When the state changes, the operating system writes the new state to those storage units which are still functioning, and to the alternate location. In order to prevent ambiguous situations, only certain defined state transitions are permitted. When the system is re-initialized, it attempts to read the state information stored on the storage units. If either unit can not be read, the system substitutes the state retrieved from the alternate state record for the state that would have been read from the non-responding unit. This pair of states from the two units index an unique entry in a state derivation table containing the resultant state.

The Hughes reference discloses a telephone dialing system uses a hand-held wand to read telephone numbers represented in bar-code form. The coded numbers are converted to electrical signals, stored and then dialed out in impulse or tone signaling form. A microprocessor implementation and its routines are described. The coded representation may be a 2-out-of-5 code or preferably a hexadecimal code provided by four bars. The hexadecimal allows the provision of characters in addition to numerals 0-9 and enables instructions and other control functions to be entered into and acted upon by the microprocessor. The telephone numbers can be provided on documents such as letterheads or directories. The instruction and control facilities can be generated from labels formed on a pad and containing the hexadecimal codes.

The Weiss reference discloses a secure registry system and method for the use thereof are provided which permits secure access to a database containing selected data on a plurality of entities, at least portions of which database has restricted access. Mechanisms are provided for controlling access to restricted access portions of the database are provided, such access being determined by at least one of the identity of the requesting entity and the entity's status. A multicharacter public code may be provided which the system can map to provide permit delivery of items, complete telephone calls and perform other functions for entities. The system may also be utilized to locate an individual based on limited biological data. Organizations utilizing the system may have custom software facilitating their access and use of the system.

Regarding claim 1, none of the cited references whether considered alone or in any combination teach or suggest a method of identifying a source of a counterfeit product unit comprising receiving a product support request from a customer, wherein the product support request relates to a product manufactured by a receiving party, receiving a technical support identification (TSID) from the customer including establishing a data communication with the customer's product unit in response to receiving the TSID and automatically interrogating the product unit to identify the TSID for the product unit, wherein at least one of a plurality of aspects of the product unit is stored in a computer retrievable location in the product unit. The method also includes validating the TSID, classifying the valid TSID as an illicit TSID classification if a unit corresponding to the TSID is identified as a counterfeit product unit including identifying the counterfeit product unit in at least one database. The method also includes assigning at least one of a plurality of support levels to the classified, valid TSID wherein the assigned support level corresponds to the TSID classification and wherein the TSID is received, validated, classified and the support level assigned before an agent is notified of the product support request and enabling delivery of the assigned support level including notifying the customer that the product unit is illicit and denying all product support, reporting at least one of the customer or the source of the counterfeit product unit and blocking access to an agent.

Regarding claim 18, none of the cited references whether considered alone or in any combination teach or suggest a system for identifying a source of a counterfeit product unit comprising an automated call distributor (ACD), wherein the ACD provides access to a customer and wherein the ACD includes a processor, a memory system coupled to the processor. Wherein the memory system includes instructions executable by the processor to receive a product support request from a customer, wherein the product support request relates to a product manufactured by a receiving party, receive a technical support identification (TSID) from the customer including establishing a data communication with the customer's product unit in response to receiving the TSID and automatically interrogating the product unit to identify the TSID for the product unit, wherein at least one of a plurality of aspects of the product unit is stored in a computer retrievable location in the product unit. The memory system includes instructions executable by the processor to validate the TSID, classify the valid TSID as an illicit TSID classification if a unit corresponding to the TSID is

identified as a counterfeit product unit including identifying the counterfeit product unit in at least one database. The memory system includes instructions executable by the processor to assign at least one of a plurality of support levels to the classified, valid TSID wherein the assigned support level corresponds to the TSID classification and wherein the TSID is received, validated, classified and the support level assigned before an agent is notified of the product support request and enable delivery of the assigned support level including notifying the customer that the product unit is illicit and denying all product support, reporting at least one of the customer or the source of the counterfeit product unit and blocking access to an agent.

None of the cited references whether considered alone or in any combination teach or suggest a method of identifying a source of a counterfeit product unit. Further, none of the cited references whether considered alone or in any combination teach or suggest *reporting at least one of the customer or the source of the counterfeit product unit*. Nothing in Edinger or Thomson discuss reporting the customer or the source of a counterfeit product such as to a third party for further investigation and action as described in Applicant's specification at paragraph 25 which provides in pertinent part:

> ...In one embodiment, the ***illicit TSIDs can be exported to other databases and other entities for follow-up, such as reports could be made to Business Software Alliance for further investigation***. Reports could also be sent to other similar internal or external entities for researching illicit hardware and software users ... (Emphasis added)

Examiner admits that in his view, Edinger neither teaches nor suggests that Edinger's system actually does perform the feature of "automatically interrogating the product unit to identify the TSID for the product unit".

Further, Edinger relies on a customer service person to manually enter the TSID data and to execute the verification. This further teaches away from Applicant's concept that of receiving "a technical support identification (TSID) from the customer including establishing a data communication with the customer's product unit and ***automatically*** interrogating the unit to identify the TSID for the unit".

The Examiner relies on Levi to teach "automatically interrogating the product unit to identify an ID for the product unit".

Applicant traverses this interpretation of Levi as follows. Levi's device identifier is used to identify the product being supported. Levi's device identifier is generated in two ways. The first way is described in the following excerpts from Levi:

> "User identifier 47 uniquely identifies each human user 45 associated with remote device monitoring system 10. User identifier 47 has an associated password, access set and may have other information, such as a user name and an office location, associated therewith. The password, access set and other information are stored in database 60. The access set defines the level of access to sites 14, site families 24 and devices 30 of the associated user 45. In particular, the access set defines the status of user 45 as a device administrator 100 (described in more detail in FIG. 3), the site administrator 140 (described in more detail in FIG. 4), a technical administrator 220 (described in more detail in FIG. 8) or a technician 221 (described in more detail in FIG. 8). Each user 45 may have one or more of the above statuses associated therewith. ***The access set is stored in database 60 and may define the user's 45 access by, for example, storing device identifiers and site identifiers associated with the devices 30 and sites 14,*** respectively, the user 45 is allowed to access. The access set may also associate the level of access permitted to the user 45 for each device and site identifier associated with the user 45 such as being site administrator 140 with full read and write access to all devices 30 associated with the site 14." (Col 7, ln 36-59, emphasis added)

> "Proceeding to block 72, after the user 45 has provided the user identifier 47 and password from block 56, the user 45 may receive a second web page having a ***device information form which the user may fill out for one or more devices 30*** that the user wishes to have tracked and monitored by remote device monitoring system 10. *Typically, the device information is provided by the user 45 with site administrator 140 or device administrator 100 access.* Device administrator 100 is typically the user 45 of the particular device 30 being signed-up for monitoring, or someone who regularly uses that device 30. A license is required for each device 30 to be tracked and monitored. The ***device information form*** may request the following information:" (Col 8, ln 19-31, emphasis added)

General Information:

Owner First Name: _____

Owner Last Name: _____

Machine Name: _____

Office Number: _____

Email Address: _____

Address 1: _____

Address 2: _____

City: _____

State: _____

Zip: _____

Reporting Information:

Do you want us to email you an event log for this device? _____

If so, how often? Weekly, monthly, quarterly, never

Email Address for Log: _____

Notes: _____

"The completed device information form is then submitted to a device table 66 portion of database 60 and, at block 74, a device identifier is generated. The device identifier generated in block 74 is also stored in device table 66. At block 75 the device identifier is provided to user 45 who is identified as site administrator 140 of the site having the just registered device 30. The device identifier may be provided to site administrator 140 by electronic mail and message board 93." (Col 8, ln 58-66)

Levi's first way of generating a device identifier is based on information contained on a ***manually filled-out device information form*** that is then submitted to the entity providing the device support where the information on the manually filled out device information form is stored in a database by the support provider ***for later use*** such as when a customer requests support for the identified device (See Levi Col 7, ln 36-59, Col 8, ln 19-66).

Levi's manual device information form process ***is not an automatic interrogation*** of the product unit and therefore is not the same as nor suggestive of Applicant's "automatically interrogating the product unit to identify an ID for the product unit".

The second way Levi's device identifier is generated is described in the following excerpts from Levi:

"Alternatively, device identifier may be generated ***automatically***. A seed application is distributed to support automatic device identification generation. The seed application is described in more detail in association with FIG. 11. The seed application comprises an executable application which may be deployed via electronic mail, electronic file transfer over a network, physical distribution, such as on a disk or CD-ROM, or by any other suitable method. Once the seed application is received at device 30, the ***seed application executes to generate a device identifier. A device identifier is generated by the seed using one or more of a device serial number associated with device 30, a desktop management interface (DMI) address, a network interface card (NIC) address, such as a MAC address, a serial number associated with the central processing unit (CPU) such as that used on the Intel Pentium III processor by Intel Corporation of Santa Clara, Calif.*** The seed process may also be distributed with a preset device identifier to be associated with device 30. Device 30 then transmits the generated device identifier to operation center 12 over Internet 34 to be stored in device table 66. The device identifier may then be provided to site administrator 140 and/or device administrator 100 by electronic mail and message board 93." (Col 8, ln 66-Col 9, ln 20)

"FIG. 11B is a flowchart illustrating a method for generating a device identifier for a particular monitored device 630 and beaconing information to operations center from the particular monitored device 630. The method begins at step 900 where seed 636 is deployed to monitored device 630. In the disclosed embodiment, deploying seed 636 comprises receiving seed 636 via electronic mail and installing seed 636 on monitored device 630. Alternatively, seed 636 may be deployed by being downloaded from a server on a local area network (LAN), by being downloaded over Internet 34, by being provided on a magnetic disk or a CD-ROM, and by any other suitable method. Next, at step 902, the device identifier associated with monitored device 630 is generated by seed 636. ***The device identifier is generated using a predetermined algorithm for yielding a unique value for the device 630 using any one of a serial number associated with device 630, the serial number associated with the Intel Pentium.RTM. III processor by Intel Corporation of Santa Clara, Calif., a desktop management interface (DMI) address, a network interface card (NIC) address and by any other suitable method.*** The device identifier may also be manually assigned by operations center 12 or by an administrator 100 or 140. The method used for generating the device identifier is stored in service parameters 740." (Col 25, ln 47-Col 26 ln 3)

Levi's second way of generating a device identifier is based on information collected by a "seed application" that is installed in the device and then "executes to generate a device identifier". The device identifier is then generated by the seed application using one or more of a device serial number associated with device 30, a desktop management interface address, a network interface card address or a serial number associated with the CPU and the generated device identifier is then delivered

to the support provider and entered into their database ***for later use*** (See Levi Col 8, ln 66-Col 9, ln 20 and Col 25, ln 47-Col 26 ln 3, Fig 11B).

Levi's second process in not the same as Applicant's "automatically interrogating the product unit to identify an ID for the product unit" because Levi's "seed application" must be installed and executed ***before*** the product support request is created so that the device identifier can be generated and then stored in the support provider's database.

Levi's second process ***requires*** that the support provider's database ***must*** have the device identifier ***before*** the product support request is generated so that when the product support request is received by the support provider, because the support provider can query their database to determine what support can be provided.

In sharp contrast, Applicant's system and method receive "a technical support identification (TSID) from the customer including establishing a data communication with the customer's product unit ***in response to receiving*** the TSID" and not before the TSID is received.

Applicant also submits that Levi's seed application is distributed in the various manners described in Levi is not the same as "establishing a data communication with the customer's product unit ***in response to receiving*** the TSID" because Levi requires that the seed application must be distributed and executed on the device before the TSID was sent.

Further, Levi's seed application is not the same as Applicant's "establishing a data communication with the customer's product unit" because Levi's seed application must be installed in the device and once it is installed and executed to generate the device identifier, the seed application has no purpose and does not communicate with the service provider or establish communications with the service provider.

Examiner relies on various other references in combination with Edinger to correct the defects in Edinger, however Applicant submits that, none of the cited references correct the deficit on Edinger as described above.

Accordingly, Applicant respectfully submits that Applicant's invention as claimed in claims 1 and 18 is patentably distinct over Edinger and any of the other cited references whether considered alone or in combination. Further, claims 3-6, 8-14, 16, 17 and 19-23 depend from one of claims 1 and 18 and are patentably distinct over the Edinger and the other cited references for at least the same reasons set forth for claims 1 and 18. Applicant therefore submits that Applicant's invention as claimed in claims 1, 3-6, 8-14 and 16-23 are patentable over Edinger and any combination of the other cited references, and respectfully request the withdrawal of the rejection under 35 U.S.C. §103(a).

SUMMARY

In view of the foregoing amendments and remarks, Applicant respectfully submits that the pending claims are in condition for allowance. Applicant respectfully requests reconsideration of the application and allowance of the pending claims.

If the Examiner determines the prompt allowance of these claims could be facilitated by a telephone conference, the Examiner is invited to contact George B. Leavell at (408) 774-6923.

Deposit Account Authorization

Authorization is hereby given to charge our Deposit Account No. 50-0805 (Ref ADAPP227) for any charges that may be due or credit our account for any overpayment. Furthermore, if an extension is required, then Applicant hereby requests such extension.

Respectfully submitted,

MARTINE PENILLA & GENCARELLA, LLP

Dated: Oct 10, 2008

George B. Leavell
Attorney for Applicant
Registration No. 45,436
710 Lakeway Drive, Suite 200
Sunnyvale, CA 94085
(408)774-6923